Hewlett Packard Enterprise

HPE Network Node Manager i Software

Software Version: 10.30
for the Windows® and Linux® operating systems

HPE Network Node Manager i Software–HPE Intelligent Management Center Integration Guide

Document Release Date: June 2017
Software Release Date: June 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, see the license-agreements directory on the NNMi product DVD.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Apple is a trademark of Apple Computer, Inc., registered in the U.S. and other countries.

AMD is a trademark of Advanced Micro Devices, Inc.

Google™ is a registered trademark of Google Inc.

Intel®, Intel® Itanium®, Intel® Xeon®, and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Internet Explorer, Lync, Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Red Hat® Enterprise Linux Certified is a registered trademark of Red Hat, Inc. in the United States and other countries.

sFlow is a registered trademark of InMon Corp.

UNIX® is a registered trademark of The Open Group.

Acknowledgements

This product includes software developed by the Apache Software Foundation. (http://www.apache.org).

This product includes software developed by the Visigoth Software Society (http://www.visigoths.org/).

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=.

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

Support

Visit the HPE Software Support web site at: **https://softwaresupport.hpe.com**

This web site provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software Support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to **https://softwaresupport.hpe.com** and click **Register**.

To find more information about access levels, go to:
https://softwaresupport.hpe.com/web/softwaresupport/access-levels

Contents

Integrate NNMi with HPE Intelligent Management Center

HPE Network Node Manager i Software (NNMi) enables you to quickly detect, isolate, and troubleshoot abnormal network behavior. Using NNMi, you can also record what has been done to date to troubleshoot or resolve a problem.

When HPE Networking devices are installed in your network, you can combine NNMi with HPE Intelligent Management Center (HPE IMC) using the HPE NNMi - HPE IMC integration. The result is a better solution for managing your enterprise network. HPE IMC adds change, configuration, and compliance features along with add-on modules for other device management needs.

For information about purchasing NNMi and HPE IMC, contact your HPE sales representative.

This document contains the following topics:

HPE NNMi - HPE IMC Integration

Use NNMi and the HPE NNMi - HPE IMC integration to leverage the features of NNMi and HPE IMC together.

Use the set of instructions, shown in "Installing, Enabling and Configuring the HPE NNMi - HPE IMC Integration" on the next page, to implement this approach. Together, NNMi and HPE IMC provide better tools to manage networks with heterogeneous elements that require highly scalable and fully integrated network management tools.

Using the HPE NNMi - HPE IMC integration provides the following functionality:

- Displays HPE IMC fault events in NNMi.
- Displays H3C device information in NNMi.
- You can launch theHPE IMC console from within NNMi to obtain H3C device details.
- Synchronizes the NNMi topology with the IMC inventory by using the IMC inventory as seeds for NNMi.
- Displays analysis panes so you can view device information.

Value

The NNMi–HPE Intelligent Management Center integration provides the following benefits:

- You see a consolidated and correlated list of network events and notifications, resulting in better root-cause analysis and reduced meant time to repair (MTTR).

- You see a comprehensive inventory, augmented by HPE IMC's rich model of H3C devices.
- You use one tool to monitor and manage your heterogenous network.
- You see a synchronized and consistent view of the network that enables self documentation and automation and reduces the total cost of ownership of your network.

Integrated Products

The information in this chapter applies to the following products:

- HPE Intelligent Management Center

  TIP: For the list of supported versions, see the NNMi Support Matrix.

- NNMi 10.30

Documentation

This document describes how to configure and use the integration.

Obtain and read the HPE IMC manuals to prepare for installing and configuring the HPE NNMi - HPE IMC integration.

Installing, Enabling and Configuring the HPE NNMi - HPE IMC Integration

After you complete "Task 1: Installing NNMi" below through "Task 4: Enabling and Configuring the HPE NNMi - HPE IMC Integration" on page 9, HPE IMC and NNMi begin sharing device information.

Steps to Install and Enable the HPE NNMi - HPE IMC Integration

Task 1: Installing NNMi

Install NNMi 10.30. To assist you with this task, point your browser to https://softwaresupport.hpe.com/ and download an interactive version of the *Network Node Manager i Installation Guide*.

Task 2: Loading the MIBs Supported by HPE IMC (Optional)

Although not mandatory, manually loading the MIBs supported by HPE IMC extends NNMi's monitoring capabilities. For example, having this additional information enables you to create custom collections using NNMi. See *Managing MIBs* in the *NNMi Help* for more information.

During the NNMi 10.30 installation, the MIBs supported by HPE IMC are *installed* on the NNMi management server. Complete the following steps to manually load these installed MIBs into NNMi using the `nnmloadmib.ovpl` script:

1. All of the NNMi processes must be running before you attempt to load any additional MIBs.
2. Look in the following directories and locate the additional MIBs that you want to load to support the HPE NNMi - HPE IMC integration:

   Windows:

   - `%NNM_SNMP_MIBS%\Vendor\H3C`
   - `%NNM_SNMP_MIBS%\IMC`

   Linux:

   - `$NNM_SNMP_MIBS/Vendor/H3C`
   - `$NNM_SNMP_MIBS/IMC`

3. To load the additional MIBs for devices supported by HPE IMC that exist in your network, see the directories shown in "All of the NNMi processes must be running before you attempt to load any additional MIBs." above. Run the following commands to load any of the MIBs for devices supported by HPE IMC. Make sure to verify that the displayed results include the MIBs you load:

   Windows:

   `nnmloadmib.ovpl -load %NNM_SNMP_MIBS%\Vendor\H3C\<mib name> -u <username> -p <password>`

   `nnmloadmib.ovpl -load %NNM_SNMP_MIBS%\IMC\<mib name> -u <username> -p <password>`

   Linux:

   `nnmloadmib.ovpl -load $NNM_SNMP_MIBS/Vendor/H3C/<mib name> -u <username> -p <password>`

   `nnmloadmib.ovpl -load $NNM_SNMP_MIBS/IMC/<mib name> -u <username> -p <password>`

   TIP: Check for prerequisite MIBs before using the **`nnmloadmib.ovpl`** script to load these MIBs. The commands shown in this step will not load the MIBs if the prerequisite MIBs are not loaded.

   Instead of using the **`nnmloadmib.ovpl`** script to load these MIBs, use the **Tools** > **Load/Unload MIB** menu in the NNMi console, as it lists any prerequisite MIBs.

4. Verify that the MIBs loaded correctly, by doing one of the following:
   - Enter the following command:

     `nnmloadmib.ovpl -list -u <username> -p <password>`

   - From the NNMi console, navigate to **Configuration** > **MIBs** > **Loaded MIBs**.

Verify the presence of the MIBs you loaded from "To load the additional MIBs for devices supported by HPE IMC that exist in your network, see the directories shown in "All of the NNMi processes must be running before you attempt to load any additional MIBs." above. Run the following commands to load any of the MIBs for devices supported by HPE IMC. Make sure to verify that the displayed results include the MIBs you load:" on the previous page.

Task 3: Loading the Trap Definitions

For NNMi to retain (not drop) HPE IMC traps, you must manually load the HPE IMC trap definitions that are important for your network. If you do not load any HPE IMC trap definitions, NNMi drops the HPE IMC traps forwarded to NNMi by HPE IMC.

NOTE: For most network environments, you will not want to load all of the HPE IMC trap definitions into NNMi. It is important that you determine the traps that are important for your network, then load only those traps into NNMi.

To load the trap definitions for HPE IMC-managed devices, do the following:

a. Change to the following directory:

- *Windows*: `%NnmInstallDir%\newconfig\HPOvNmsEvent`
- *Linux*: `$NnmInstallDir/newconfig/HPOvNmsEvent`

b. For NNMi to retain (not drop) HPE IMC traps, you must manually load the HPE IMC trap definitions that are important for your network. If you do not load any HPE IMC trap definitions, NNMi drops the HPE IMC traps forwarded to NNMi by HPE IMC.

NOTE: NNMi provides the `nnm-imc-incidentConfig.xml` file that contains thousands of the HPE IMC trap definitions. In most network environments, you do not want to load all of these trap definitions into NNMi. To stop from loading unnecessary trap definitions, create a subset of the `nnm-imc-incidentConfig.xml` file, removing any of the trap definitions you do not need.

To help determine which incidents to retain from the `nnm-imc-incidentConfig.xml` file, you might do the following:

a. Access your HPE IMC product.

b. Browse the alarms that you are receiving, and determine which IMC alarms you want to forward to NNMi.

c. Look for and save the incident definitions that contain the OIDs for those alarms in a file, such as `myincidents.xml`.

d. Use the `myincidents.xml` file in the `nnmconfigimport.ovpl` command as shown below.

In rare circumstances, you might need to load a large number of trap definitions and could experience **Configuration Import Errors**. See "Loading Trap Definitions: I need to load a large quantity of HPE IMC trap definitions and am encountering Configuration Import Errors." on page 15 for more information.

Depending on whether you decide to use the `nnm-imc-incidentConfig.xml` file or the `myincidents.xml` file, use one of the following commands to load the HPE IMC trap definitions:

- **nnmconfigimport.ovpl -f myincidents.xml -u *<username>* -p *<password>***
- **nnmconfigimport.ovpl -f nnm-imc-incidentConfig.xml -u *<username>* -p *<password>***

Task 4: Enabling and Configuring the HPE NNMi - HPE IMC Integration

After completing the steps in this section NNMi gathers data from the IMC servers you configured for the integration. During this discovery process, NNMi adds seeds for devices found in the set of IMC servers and links the devices to their IMC source.

NNMi discovers the devices contained in the IMC inventory and obtains information from IMC about these devices if they meet the following criteria:

- NNMi has not already discovered the device.
- The device is not already entered as a seed device in NNMi.

See "Discovering Information from IMC" on page 13 for more information.

To enable the HPE NNMi - HPE IMC integration, do the following:

1. From the NNMi console, click **Integration Module Configuration** > **IMC**. NNMi shows the **HPE NNMi - HPE IMC Integration Configuration** screen.
2. Select **Enable IMC Integration**.
3. Select **IMC SSL** if you configured IMC to accept SSL connections.

   NOTE: You must also complete the steps shown in "Task 5: Configuring SSL Access for the HPE NNMi - HPE IMC Integration" on the next page to manually import the HPE IMC certificate into the NNMi `truststore` file.

4. Add the following NNMi integration information:
   - `NNMi host`: This field contains the fully qualified domain name of the NNMi management server.
   - `NNMi User`: Enter an NNMi username that is mapped to an NNMi Administrators user group. This can also be an NNMi username mapped to an NNMi Web Service Clients user group.
   - `NNMi Password`: Enter the NNMi username password.
5. Add the following HPE IMC integration information:
   - `IMC host`: This field contains the fully qualified domain name of the IMC server.
   - `IMC Port`: This field contains the port number used for accessing the IMC server.
   - `IMC User`: Enter the IMC username.
   - `IMC Password`: Enter the IMC username password.
6. Optional: You can configure the HPE NNMi - HPE IMC integration module for multiple IMC servers. These IMC servers function as element managers for a set of devices. These devices would then be seeded into NNMi so that NNMi is aware of the full set of devices. To add another IM server, click **Add another IMC server**.

NOTE: You do not need to configure the same username and password on each IMC host. NNMi supports using a separate IMC host username and password for each IMC host.

7. Click **Submit** to finish enabling the HPE NNMi - HPE IMC integration. After you click **Submit**, HPE IMC and NNMi begin sharing device information.

NOTE: NNMi periodically reads the set of management IP addresses from each configured IMC server. For each device that NNMi has not already discovered, and that does not already have a NNMi seed entry, NNM adds the new device or devices to its inventory. NNMi also saves the device ID as a custom attribute on the NNMi node.

NOTE: If a node is removed from HPE IMC or NNMi, you must manually remove the node from the other application. There is no automatic discovery synchronization for removing a node from HPE IMC or NNMi.

Task 5: Configuring SSL Access for the HPE NNMi - HPE IMC Integration

After completing this task, single sign-on works between the NNMi console and the HPE IMC console. Completing this task permits you to open the HPE IMC console from the NNMi console to view the device details residing in IMC.

If you selected **IMC SSL** in "Select IMC SSL if you configured IMC to accept SSL connections." on the previous page, complete the following steps to configure an SSL connection between NNMi and HPE IMC.

NOTE: The instructions in this section include how to import the IMC trust certificate into the NNMi trust store. Before you import the IMC trust certificate into the NNMi trust store, you must replace the IMC keystore with one that you create (as shown in " a. Generate a replacement IMC keystore file using the following command. " below through " b. Replace the keystore file in the <IMC_Installation_Directory>\client\security\ directory with the keystore file you generated in " a. Generate a replacement IMC keystore file using the following command. " on the previous page." on the next page), so that the hostname verification succeeds when NNMi connects to HPE IMC.

NOTE: SSL authentication relies on certificate path validation. For example, if VeriSign guarantees NNMi, and NNMi guarantees HPE IMC, then the certificate path will be HPE IMC <- NNMi <- VeriSign and authentication works correctly. These instructions assume that most systems trust VeriSign, and that you only need to import the NNMi and HPE IMC certificates.

Important: If the HPE IMC <- NNMi <- VeriSign chain is broken due to the NNMi certificate not being imported into HPE IMC, or the HPE IMC certificate not being imported into NNMi, the SSL authentication will not work properly.

a. Generate a replacement IMC `keystore` file using the following command.

NOTE: Replace <*IMC_FQDN*> with the fully qualified domain name of the IMC server.

Windows: **<*IMC_Installation_Directory*>\deploy\jdk\jre\bin\keytool.exe -genkey -v -alias iMC -validity 3650 -keyalg RSA -dname "CN=<*IMC_FQDN*>, OU=*your_workgroup*, O=Unknown, L=Unknown, S=Unknown, C=Unknown" -keypass iMCV300R002 -storepass iMCV300R002 -keystore keystore**

Linux: **<*IMC_Installation_Directory*>/deploy/jdk/jre/bin/keytool -genkey -v -alias iMC -validity 3650 -keyalg RSA -dname "CN=<*IMC_FQDN*>, OU=*your_workgroup*, O=Unknown, L=Unknown, S=Unknown, C=Unknown" -keypass iMCV300R002 -storepass iMCV300R002 -keystore keystore**

b. Replace the `keystore` file in the <*IMC_Installation_Directory*>`\client\security\` directory with the `keystore` file you generated in " a. Generate a replacement IMC keystore file using the following command. " on the previous page.

c. Export the IMC certificates from the `keystore` file using the following command:

Windows:
<*IMC_Installation_Directory*>\deploy\jdk\jre\bin\keytool.exe -export -alias imc -file C:\temp\IMC.cer -keystore <*IMC_Installation_Directory*>\client\security\keystore -storepass iMCV300R002

Linux:
<*IMC_Installation_Directory*>/deploy/jdk/jre/bin/keytool -export -alias imc -file /tmp/IMC.cer -keystore <*IMC_Installation_Directory*>/client/security/keystore -storepass iMCV300R002

d. Verify that you see the `Certificate stored in file <directory>:\IMC.cer` message.

e. Copy the certificate from the `IMC.cer` file you created in " c. Export the IMC certificates from the keystore file using the following command:" above to the NNMi management server.

f. Open a command window on the NNMi management server.

g. To import the IMC certificate into the NNMi `nnm.truststore` file, run the following command:

Windows:
"%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe" -import -alias sentinel -file <*directory*>\IMC.cer -keystore "%NnmDataDir%\shared\nnm\certificates\nnm.truststore" -storepass ovpass

Linux:
$NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -import -alias sentinel -file <*directory*>/IMC.cer -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass

Make sure you answer **yes** when asked whether to `Trust this certificate?`. The following program listing is an example of what happens after you run this command:

```
Owner: CN=iMC Development Team, OU=R&D Beijing, O="Hangzhou H3C Technologies Co,.
Ltd.", L=Shang-Di Information Industry Base, ST=Beijing, C=CN
Issuer: CN=iMC Development Team, OU=R&D Beijing, O="Hangzhou H3C Technologies
Co,. Ltd.", L=Shang-Di Information Industry Base, ST=Beijing, C=CN
Serial number: 4609e6be
Valid from: Tue Mar 27 21:53:34 MDT 2007 until: Sun Mar 27 21:53:34 MDT 2022
Certificate fingerprints:
      MD5: A6:3D:D9:F2:15:13:09:4A:22:00:D9:C1:35:CD:53:02
      SHA1: 3D:40:80:73:C8:32:FA:23:F5:24:02:2D:6B:D9:12:C2:DA:94:66:85
      Signature algorithm name: MD5withRSA
      Version: 1
```

```
Trust this certificate? [no]: yes
Certificate was added to keystore
```

h. Obtain the NNMi certificate alias name using the following command. Write down the alias value obtained during this step, as you will need that value for the `<alias>` variable used during the next step.

Windows:

"%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe" -v -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore" -storepass nnmkeypass

Linux:

<NnmInstallDir>/nonOV/jdk/hpsw/bin/keytool -v -list -keystore <NnmDataDir>/OV/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass

i. Export the NNMi certificate to a file using the following command.

Windows:

"%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe" -export -alias <alias> -file <directory>\nnm.cer -keystore %NNMDataDir%\shared\nnm\certificates\nnm.keystore -storepass nnmkeypass

Linux:

<NnmInstallDir>/nonOV/jdk/hpsw/bin/keytool -export -alias <alias> -file <Directory>/nnm.cer -keystore <NnmDataDir>/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass

j. Copy the NNMi certificate file to a directory on the IMC server.

> **NOTE:** For multiple IMC servers, complete " j. Copy the NNMi certificate file to a directory on the IMC server." above through " l. Restart the IMC server using the HPE Intelligent Deployment Monitoring Agent." on the next page for each IMC server you plan to use in the HPE NNMi - HPE IMC integration.

k. Import the NNMi certificate to the IMC `truststore` file using the following command.

Windows:

<*IMC_Installation_Directory*>\deploy\jdk\jre\bin\keytool.exe -import -alias <alias> -file <Directory>\nnm.cer -keystore <*IMC_Installation_Directory*>\iMC\client\security\truststore -storepass iMCV300R002

Linux:

<*IMC_Installation_Directory*>/deploy/jdk/jre/bin/keytool -import -alias <alias> -file <Directory>/nnm.cer -keystore <*IMC_Installation_Directory*>/iMC/client/security/truststore -storepass iMCV300R002

Make sure you answer **yes** when asked whether to `Trust this certificate?`. The following program listing is an example of what happens after you run this command:

```
Owner: CN=<fully qualified system name>
Issuer: CN=<fully qualified system name>
Serial number: 50789c62
Valid from: Fri Oct 12 16:40:34 MDT 2012 until: Sun Sep 18 16:40:34 MDT 2112
Certificate fingerprints:
```

```
        MD5: CA:10:C4:8E:88:D5:21:04:DC:F2:95:74:47:65:B5:82
        SHA1: 0B:8D:1D:3F:F0:AA:87:87:D9:E9:1C:CD:DA:4F:C1:62:BF:62:E1:03
        Signature algorithm name: SHA1withRSA
        Version: 3
    Trust this certificate? [no]: yes
    Certificate was added to keystore
```

l. Restart the IMC server using the HPE Intelligent Deployment Monitoring Agent.

m. Run the following command sequence on the NNMi management server:

- **ovstop**
- **ovstart**

n. *Optional*: Run the following commands on both the NNMi management server and the IMC server. Compare the outputs to make sure the keystore certificates reside on both servers' truststore files:

NNMi management server (Windows):
keytool.exe -v -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm.truststore -storepass ovpass

NNMi management server (Linux):
keytool -v -list -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass

IMC server (Windows):
<*IMC_Installation_Directory*>\deploy\jdk\jre\bin\keytool.exe -v -list -keystore <*IMC_Installation_Directory*>/iMC/client/security/truststore -storepass iMCV300R002

IMC server (Linux):
<*IMC_Installation_Directory*>/deploy/jdk/jre/bin/keytool -v -list -keystore <*IMC_Installation_Directory*>/iMC/client/security/truststore -storepass iMCV300R002

Discovering Information from IMC

During discovery, NNMi gathers data from the IMC servers you configured for the integration. During this discovery process, NNMi adds seeds for all the devices found in the set of IMC servers and links the devices to their IMC source. NNMi also saves the device ID as a custom attribute on the NNMi node.

During discovery, if there are devices that have been discovered by multiple IMC servers, NNMi links the first IMC server reporting these devices as the IMC source. If multiple IMC servers discover a device, then NNMi only discovers the device from the first IMC server reporting the device to NNMi.

Devices contained in the IMC inventory share information with NNMi if they meet the following criteria:

- NNMi has not already discovered the device.
- The device is not already listed as a seed address in NNMi.

If NNMi has already discovered nodes that also reside in the IMC database, NNMi does not automatically update `customAttributes` for these devices. To make configuration changes so NNMi automatically updates customAttributes for devices found in IMC, see "Discovery Configuration Change: Make configuration changes so NNMi automatically updates customAttributes for devices found in IMC." on page 15.

Using the HPE NNMi - HPE IMC Integration

Opening an IMC console from a Node in NNMi

If you select any node in NNMi that was seeded from an IMC server, you can use the **HPE IMC**->**View node in IMC** menu from the NNMi console to open the IMC console. From the IMC console, you can log on to view information about the selected node. If you configured SSL access for the HPE NNMi - HPE IMC Integration, the **HPE IMC**->**View node in IMC** menu in the NNMi console takes you directly to the device view in the corresponding IMC console.

NOTE: The **HPE IMC**->**View node in IMC** menu item is enabled only if the selected node is *SNMP enabled*.

To open an IMC console view from the NNMi console (of any node that was seeded from an IMC server), complete these steps:

1. Use the **Action** > **HPE IMC** > **View Node in IMC** menu to open a view of the node in the HPE IMC console.
2. You can also use nodes located in Topology Maps in the NNMi console to access theHPE IMC console: for example, select a node from a Layer 3 Neighbor view; then right-click the node and use the **HPE IMC** > **View Node in IMC** to open a view of the node in the HPE IMC console.

Using the Analysis Pane to View Device Information

When using the HPE NNMi - HPE IMC integration, the NNMi console includes two additional analysis panels. These panels show device information when a selected node originates from an IMC server. These two panels are labeled **Asset Details** and **Hardware/Firmware**. Select **Asset Details** to view a table of HPE IMC-monitored device components. Select **Hardware/Firmware** to view additional hardware and firmware details discovered by HPE IMC.

NOTE: The menu option is disabled for non-IMC nodes OR for non-SNMP nodes (even if they came from IMC).

Disabling the HPE NNMi - HPE IMC Integration

To disable the HPE NNMi - HPE IMC integration, do the following:

1. From the NNMi console, click **Integration Module Configuration** > **IMC**. NNMi shows the **HPE NNMi - HPE IMC Integration Configuration** screen.
2. Deselect **Enable IMC Integration**.
3. Click **Submit** to finish disabling the HPE NNMi - HPE IMC integration.

> **NOTE:** If you disable the HPE NNMi - HPE IMC integration, then enable the integration at a later time, the discovery process starts again (re-synchronizes) to ensure that NNMi has the latest device information from the IMC servers.

After you disable the HPE NNMi - HPE IMC integration, log out of the NNMi console, then log back in, you will no longer see the IMC-related menu items in the NNMi console. There are no other user actions required after completing these steps.

Maintaining the HPE NNMi - HPE IMC Integration

Loading Trap Definitions: I need to load a large quantity of HPE IMC trap definitions and am encountering *Configuration Import Errors*.

Solution: Although HPE discourages loading all of the IMC incident definitions discussed in "Task 3: Loading the Trap Definitions" on page 8, there might be rare situations that require you to load many of the IMC incident definitions. If you must load a large number of trap definitions, split the **`nnm-imc-incidentConfig.xml`** file into two or more separate files, each containing a subset of the trap definitions, then load each file separately.

Discovery Configuration Change: Make configuration changes so NNMi automatically updates customAttributes for devices found in IMC.

Required Configuration Changes: NNMi will not automatically update customAttributes for devices found in IMC if these devices already reside in the NNMi database. To configure the HPE NNMi - HPE IMC integration to automatically update customAttributes for devices found in IMC, do the following:

1. Remove the seeds for the devices from NNMi. To do this use the **Configuration** > **Discovery** > **Seeds** menu.
2. Delete the node from NNMi:
   a. Use the **Inventory** > **Nodes** menu.
   b. Select the nodes you want to delete.
   c. Use the **Action** > **Delete** menu to delete the nodes.
3. NNMi now receives information about the deleted devices, including `customAttributes`, from IMC.
4. NNMi rediscovers the device using information forwarded by IMC.

> **NOTE:** NNMi might not initiate a discovery for 24 hours, so the nodes might not be seeded in NNMi for some time, unless you disable, then enable the configuration.

If you delete any nodes that NNMi assigned to tenants other than the **Default Tenant**, then NNMi will rediscover those nodes and assign them to the Default Tenant. This Default Tenant assignment could disrupt

an NNMi tenant model configuration. See *NNMi Security and Multi-Tenancy* in the *NNMi Deployment Reference*.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on HPE Network Node Manager i Software—HPE Intelligent Management Center Integration Guide (Network Node Manager i Software 10.30)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to network-management-doc-feedback@hpe.com.

We appreciate your feedback!